数理解析研究所講究録
273巻 1976年 198-205

Some Remarks on Abelian Varieties

東大 理　　塩田徹治

§0. アーベル多様体に関する次の問題を考える：

問題1. アーベル多様体 A とその部分アーベル多様体 B_1, B_2 が与えられたとき、商アーベル多様体 A/B_i について、

$$B_1 \simeq B_2 \Longrightarrow A/B_1 \simeq A/B_2 \quad ?$$

問題2. A, A' を代数体 K 上定義されたアーベル多様体とし、K の素イデアル $\mathfrak{p}$ について、A, A' の reduction mod $\mathfrak{p}$ をそれぞれ $A(\mathfrak{p})$, $A'(\mathfrak{p})$ とかく。このとき、もし $A \not\simeq A'$ (K の代数的閉体の上で) ならば、$A(\mathfrak{p}) \simeq A'(\mathfrak{p})$ となる $\mathfrak{p}$ は高々有限個にかぎられるか？

問題1の特別な場合として、楕円曲線 E, E', E'' について次の問を発することができる ("Cancellation problem")：

問題3. $E \times E' \simeq E \times E'' \Longrightarrow E' \simeq E''$?

問題4. $E \times E \simeq E \times E' \Longrightarrow E \simeq E'$?

さて、答はいずれも一般には否定的である！ それを示す

のが本稿の目的である。明らかに問題３又は４の反例は問題１の反例を与えるから、我々は主として直積型のアーベル曲面，即ち $A = E \times E'$（E, E'：楕円曲線）の形のものを考察する。問題２に関しても このような A, A' から反例を見出すことができる。

まずアーベル曲面 $A = E \times E'$ のピカール数 ρ について、次の事実を思出す（cf. [1], Appendix）

$$\rho(A) = \begin{cases} 2 & E \not\sim E' \\ 3 & E \sim E', \quad \mathrm{End}(E) = \mathbb{Z} \\ 4 & E \sim E', \quad \mathrm{End}(E) \simeq \mathbb{Z}^2 \\ 6 & E \sim E', \quad \mathrm{End}(E) \simeq \mathbb{Z}^4 \end{cases}.$$

ここで、$\sim$ は同種，$\mathrm{End}(E)$ は E の自己準同型環をあらわす。

<u>命題</u>．もし $\rho(E \times E') \leq 3$ ならば 問題３（及び４）は正しい。

証明は省略する。一般の場合の結果は次の通り：

標数	問題３	問題４
0	No	Yes
$p>0$	No $\Leftarrow$	No

標数 $p > 0$ のとき、４の反例を supersingular な E を用いて構成する。標数０（複素体上）の場合、特異アーベル曲面の理論（[2]）を応用して、単に反例を与えるのみならず、問題３の完全な理解が可能である。

§1. まず問題4の標数 $p>0$ における反例をあげる：

例I $p \equiv 3 \pmod 4$，$k = \mathbb{F}_{p^2}$ とし，次の楕円曲線を考える

(1) $E: \quad Y^2 = X^3 - X$.

(2) $E': \quad \eta^2 = (\xi+1)(\xi^2 - 4\xi - 4)$.

このとき $E \times E \simeq E \times E'$ (k上) であるが，

$p \geq 7$ なら $E \not\simeq E'$ (kの閉体$\bar{k}$上でも) である。

次に 問題2の反例：

例II 上の楕円曲線 E および E' を Gaussの数体 $\mathbb{Q}(\sqrt{-1})$ の上で考え アーベル曲面

(3) $A = E \times E$, $A' = E \times E'$

を考える。このとき

(4) $A \not\simeq A'$ ($\mathbb{C}$上)

(5) $A \bmod p \simeq A' \bmod p$, $\forall p \equiv 3 \pmod 4$.

これらを示すために，まず上のEを一般の体k上で考える。Eに無限遠点を原点Oとして群の構造を入れると，2等分点は $v: (X, Y) = (0, 0)$ および $w: (X, Y) = (1, 0)$ で生成される。簡単な計算により，点vまたはwによるE上の平行移動は夫々

$(X, Y) \longrightarrow (-1/X, \ Y/X^2)$,

$(X, Y) \longrightarrow ((X+1)/(X-1), \ -2Y/(X-1)^2)$

で与えられる。従って これらによる商曲線 $E/\langle v \rangle$, $E/\langle w \rangle$ について $E/\langle v \rangle \simeq E$, $E/\langle w \rangle \simeq E'$ が容易に確められる。一方 不変量をみると

$$j(E) = 2^6 \cdot 3^3 \quad , \quad j(E') = (2 \cdot 3 \cdot 11)^3$$

だから $E \simeq E'$ ($\bar{k}$上) となるのは $p = 3$ 又は 7 に限る。

さて よく知られているように

$$E : \text{supersingular} \iff p \equiv 3 \pmod 4 .$$

しかも このとき $k \ni \sqrt{-1}$ とする (i.e. $k \supset \mathbb{F}_{p^2}$) と E の k上有理的な自己準同型の環 $\mathrm{End}_k(E)$ は rank 4 の加群となる。

そこで 例Iを証明するには 次の事が成立てば十分である:

アーベル曲面 $E \times E$ の k上の自己同型(群の意味でも)で点 (v, o) を点 (o, w) に写すものが存在する。

実際 これを認めると $E \times E$ を これらの2等分点で割って

$$(E/\langle v \rangle) \times E \simeq E \times (E/\langle w \rangle) \quad (k \text{上})$$

従って $E \times E \simeq E \times E'$ (k上) を得る。

補題 一般に E を 標数 p の supersingular な楕円曲線, $\ell \neq p$ を素数, v, w を E の ℓ等分点の群 E_ℓ の生成元とする。このとき $\mathrm{Aut}(E \times E) \ni f$ で $f(v, o) = (o, w)$ となるものが存在する。さらに $\mathrm{End}_k(E) \simeq \mathbb{Z}^4$ かつ v, w が k上有理的なら f として k-有理的なものがとれる。

証明. Eの準同型を, ℓ等分点の群 E_ℓ に制限することにより. 自然な群の準同型

$$r: \quad \mathrm{End}_k(E) \longrightarrow \mathrm{End}(E_\ell)$$

が生ずる。$\mathrm{Ker}(r) \ni \varphi \iff \varphi(x)=0, \ \forall x \in E_\ell \iff \varphi = \ell\cdot\psi$, $\exists \psi \in \mathrm{End}_k(E)$, だから.

$$\bar{r}: \quad \mathrm{End}_k(E)/\ell\cdot\mathrm{End}_k(E) \hookrightarrow \mathrm{End}(E_\ell)。$$

ところが仮定より. どちらも $\mathbb{Z}/\ell$ (素体) 上 4次元のベクトル空間だから $\bar{r}$ は同型. 従って. r は全射となる。

さて. v, w は E_ℓ の ($\mathbb{Z}/\ell$ 上の) 底であるから. $\mathrm{End}(E_\ell)$ の元で $v \mapsto w$, $w \mapsto 0$ なるものが存在する。上の注意から

$$\exists \varphi \in \mathrm{End}_k(E), \quad \varphi(v)=w, \quad \varphi(w)=0.$$

同様にして

$$\exists \psi \in \mathrm{End}_k(E), \quad \psi(v)=0, \quad \psi(w)=v.$$

そこで. $E\times E$ の自己同型 f_1, f_2 を次の様に定義する:

$$f_1(x, y) = (x, y+\varphi(x))$$

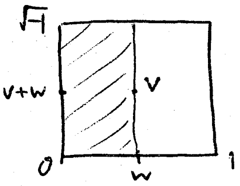
$$f_2(x, y) = (x+\psi(y), y).$$

このとき $f_1(v, 0) = (v, w) = f_2(0, w)$ だから. $f = f_2^{-1}\circ f_1$ とおくと. f は補題の条件をみたす。 証終.

以上で. 例Iが示された。例IIについては. あと. (4)を示せば十分である。

複素数体 $\mathbb{C}$ 上で、楕円曲線(1), (2) は、夫々、次の複素トーラスと同一視される。

$$E \simeq \mathbb{C}/(\mathbb{Z}+\mathbb{Z}\sqrt{-1}),$$
$$E' \simeq \mathbb{C}/(\mathbb{Z}+\mathbb{Z}\,2\sqrt{-1}).$$



実際、前者は、$\mathrm{Aut}(E) \ni \sqrt{-1}$ から明らか、後者は、$E' \cong E/\langle w\rangle$ となること（および $E/\langle v\rangle \simeq E$）から分る。

故に、(3) で定義されるアーベル曲面は、いわゆる特異アーベル曲面になる：すなわち、$\rho(A)=\rho(A')=4$.

一般に、$\mathbb{C}$ 上の特異アーベル曲面 A に対し、A 上の代数的サイクルの群 S_A は $H_2(A,\mathbb{Z})$ の rank 4 の部分加群であるから、その直交補空間として"超越的サイクル"の群 T_A が定義され rank 2 である。今 T_A の底 $\{t_1, t_2\}$ で

$$\mathrm{Im}\left(\int_{t_1}\omega \Big/ \int_{t_2}\omega\right) > 0$$

となるものをとる。ここに ω は A 上の正則な 2-form である。そして、T_A の交叉行列

$$Q_A = \begin{pmatrix} t_1 t_1 & t_1 t_2 \\ t_1 t_2 & t_2 t_2 \end{pmatrix}$$

を考えると、これは、T_A の上のような底の変換により

$$Q \longrightarrow {}^t\gamma Q \gamma \quad, \exists \gamma \in SL_2(\mathbb{Z}),$$

となる。従って、次の対応が得られた：

$$A \longmapsto \{Q_A\} \bmod SL_2(\mathbb{Z}).$$

特異アーベル曲面の理論[2]により、これは、特異アーベル曲面の同型類の集合から、正定値偶整二元二次形式の狭義同値類の集合の上への1対1の対応を与える。

さて、問題の A, A′ については、[2] p. 265～により、直ちに

$$Q_A \sim \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}, \quad Q_{A'} \sim \begin{pmatrix} 4 & 0 \\ 0 & 4 \end{pmatrix}$$

が分る。従って A と A′ は ($\mathbb{C}$ 上) 同型であり得ない。故に(4)が示され、例 II の証明は終る。

§2. 標数 0 の時、問題 3 (および 4) を考える。§0 で述べた命題により、$\rho(E \times E') \leq 3$ のときは、正しいから $\rho(E \times E') = 4$, 即ち $E \times E'$ は特異アーベル曲面の時を考えればよい。このとき、E と E′ は同種で、虚数乗法をもつ楕円曲線である。共通する虚数乗法の二次体を K とかく。

K の整数環を $\mathcal{O}$, その導手 f の order を $\mathcal{O}_f$ とかく (i.e. $\mathcal{O}_f$ は $\mathcal{O}$ の指数 f の唯一つの部分環)。さらに

$$\mathrm{End}(E) = \mathcal{O}_f, \quad \mathrm{End}(E') = \mathcal{O}_{f'},$$
$$(f, f') = d$$

とおく。この時、

<u>定理</u>. 上のように E, E′ が与えられたとき、

$$E \times E'' \simeq E \times E'$$

となる楕円曲線 E'' の同型類の個数 N は有限で 次の公式で与えられる:

$$N = h(\mathcal{O}_{f'}) / h(\mathcal{O}_d)$$
$$= (f'/d) \cdot [\mathcal{O}_d^{\times} : \mathcal{O}_{f'}^{\times}]^{-1} \prod_{p \mid (f'/d)} \left(1 - \frac{\chi(p)}{p}\right).$$

ここで $h(\mathcal{O}_{f'}), \cdots$ は $\mathcal{O}_{f'}, \cdots$ の類数, $\mathcal{O}_{f'}^{\times}$ は $\mathcal{O}_f$ の単元の群, $\chi(p) = \left(\frac{K}{p}\right)$ は K の Legendre 記号である。

(証明は §1 の最後で述べた特異アーベル曲面に関する結果により, 二次体の理論に帰着する. 詳しいことは [3] を参照されたい.)

特に $E = E'$ のときは $f = f'$ で 上の $N = 1$. 即ち 問題4 が $\mathbb{C}$ の場合成立する。($\rho(E \times E) \leq 3$ のときは §0 命題によって やはりよい)。他方 $N > 1$ となる例を与えることも容易で それは 問題3 の反例を与える.

なお こういう問題を考えた動機は Kummer 曲面に関連した問題に由来するが, それについても [3] を見られたい.

Reference

[1] T. Shioda, Algebraic cycles on certain K3 surfaces in char. p, Proc. Int. Conf. on Manifolds, Univ. Tokyo Press, 1975.

[2] —— and N. Mitani, Singular abelian surfaces and binary quadratic forms, in Springer Lecture Note 412, 1974

[3] ——, Some remarks on abelian varieties, (to appear)